Involutive Bases II

Werner M. Seiler
Institut für Mathematik
Universität Kassel

Overview

- **General Involutive Bases**
- **Basic Algorithms**
  - ☐ Continuous and Constructive Divisions
  - ☐ Monomial Completion
  - ☐ Polynomial Completion
  - ☐ Minimal Bases and Optimisations
- **Pommaret Bases and δ-Regularity**
- **Combinatorial Decompositions and Applications**
- **Syzygy Theory and Applications**

Basic Computational Problems

- existence of **finite** involutive basis
  - ☐ clear for Noetherian division via Gröbner bases. . .
  - ☐ . . . but recall counterexample for Pommaret division
- **effective** criterion for involutive basis
  - ☐ basic theory provides *no* finite test
  - ☐ need “substitute” for S-polynomials
  - ☐ where lies *“first”* obstruction to involution?
- **algorithmic** construction of involutive basis
  - ☐ non-trivial already in *monomial* case!
  - ☐ “reduced” basis — uniqueness?
- **efficient** algorithms
  - ☐ optimisations
  - ☐ heuristics

Continuous and Constructive Divisions

Idea: consider only *"nearest"* obstruction to involution ⇝ multiply with a *single* non-multiplicative variable

Def: finite set $\mathcal{T} \subset \mathbb{T}(X)$ *locally involutive* ⇝

$$\forall t \in \mathcal{T},\ y \in \bar{X}_{L,\mathcal{T}}(t)\ :\ yt \in \langle \mathcal{T} \rangle_L$$

(here: $\bar{X}_{L,\mathcal{T}}(t) = X \setminus X_{L,\mathcal{T}}(t)$ set of *non*-multiplicative variables)

Continuous and Constructive Divisions

Idea: consider only *“nearest”* obstruction to involution $\rightsquigarrow$
multiply with a *single* non-multiplicative variable

Def: finite set $\mathcal{T} \subset \mathbb{T}(X)$ *locally involutive* $\rightsquigarrow$

$$\forall t \in \mathcal{T},\ y \in \bar{X}_{L,\mathcal{T}}(t) \,:\, yt \in \langle \mathcal{T} \rangle_L$$

(here: $\bar{X}_{L,\mathcal{T}}(t) = X \setminus X_{L,\mathcal{T}}(t)$ set of *non*-multiplicative variables)

obviously: $\mathcal{T}$ involutive $\Longrightarrow$ $\mathcal{T}$ locally involutive

what about the converse?

Continuous and Constructive Divisions

Example: recall bizarre global division on $\mathbb{T}(x, y, z)$ defined in Lecture I by the following set of multiplicative variables

$$X_L(1) = \{x, y, z\}$$
$$X_L(x) = \{x, z\}, \quad X_L(y) = \{x, y\}, \quad X_L(z) = \{y, z\},$$
$$X_L(t) = \emptyset \text{ for all other } t \in \mathbb{T}(x, y, z)$$

Consider the set $\mathcal{T} = \{x, y, z\}$

- $\mathcal{T}$ *locally* involutive

$$y \cdot x = x \cdot y \qquad z \cdot y = y \cdot z \qquad x \cdot z = z \cdot x$$

- But $\mathcal{T}$ *not* involutive: $xyz \in \langle \mathcal{T} \rangle \setminus \langle \mathcal{T} \rangle_L$

Continuous and Constructive Divisions

Def: involutive division L *continuous* $\rightsquigarrow$

$$\forall \text{ finite sets } \mathcal{T} \subset \mathbb{T}(X) \quad \forall \text{ finite sequences } (t_1, \dots, t_r)$$

$$\text{with } \ t_i \in \mathcal{T} \text{ and } \ \forall t_i \, \exists y_i \in \bar{X}_{L,\mathcal{T}}(t_i) \ : t_{i+1} \,|_{L,\mathcal{T}}\, y_i t_i$$

$$\forall k \neq \ell \ : \ t_k \neq t_\ell$$

(in other words: such sequences cannot be *cyclic*)

Continuous and Constructive Divisions

Def: involutive division L *continuous* $\rightsquigarrow$

$$\forall \text{ finite sets } \mathcal{T} \subset \mathbb{T}(X) \quad \forall \text{ finite sequences } (t_1, \dots, t_r)$$

$$\text{with } \; t_i \in \mathcal{T} \text{ and } \; \forall t_i \, \exists y_i \in \bar{X}_{L,\mathcal{T}}(t_i) \;:\; t_{i+1} \,|_{L,\mathcal{T}}\, y_i t_i$$

$$\forall k \neq \ell \;:\; t_k \neq t_\ell$$

(in other words: such sequences cannot be *cyclic*)

Prop: L continuous, $\mathcal{T}$ locally involutive $\Longrightarrow$ $\mathcal{T}$ involutive

(provides us with *finite* criterion for involutive sets!)

Continuous and Constructive Divisions

Def: involutive division L *continuous* $\rightsquigarrow$

$$\forall \text{ finite sets } \mathcal{T} \subset \mathbb{T}(X) \quad \forall \text{ finite sequences } (t_1, \dots, t_r)$$

$$\text{with } t_i \in \mathcal{T} \text{ and } \forall t_i \, \exists y_i \in \bar{X}_{L,\mathcal{T}}(t_i) \; : t_{i+1} \mid_{L,\mathcal{T}} y_i t_i$$

$$\forall k \neq \ell \; : \; t_k \neq t_\ell$$

(in other words: such sequences cannot be *cyclic*)

Prop: L continuous, $\mathcal{T}$ locally involutive $\Longrightarrow$ $\mathcal{T}$ involutive

(provides us with *finite* criterion for involutive sets!)

Proof: (quite technical)
assume existence of *minimal* obstruction to involution x^μ *not* of form yt; starting from divisor $t \in \mathcal{T}$ of x^μ, construct infinite sequence contradicting continuity of division L

Continuous and Constructive Divisions

Def: involutive division L *continuous* $\rightsquigarrow$

$$\forall \text{ finite sets } \mathcal{T} \subset \mathbb{T}(X) \quad \forall \text{ finite sequences } (t_1, \dots, t_r)$$

$$\text{with } \ t_i \in \mathcal{T} \text{ and } \ \forall t_i\, \exists y_i \in \bar{X}_{L,\mathcal{T}}(t_i) \ : t_{i+1} \,|_{L,\mathcal{T}}\, y_i t_i$$

$$\forall k \neq \ell \ : \ t_k \neq t_\ell$$

(in other words: such sequences cannot be *cyclic*)

Prop: L continuous, $\mathcal{T}$ locally involutive $\Longrightarrow$ $\mathcal{T}$ involutive

(provides us with *finite* criterion for involutive sets!)

Lemma: Janet and Pommaret division continuous

Proof: sequence ascending in appropriate sense

Janet division $\rightsquigarrow$ $\prec_{\text{lex}}$

Pommaret division $\rightsquigarrow$ “essentially” $\prec_{\text{revlex}}$

Continuous and Constructive Divisions

Problem: continuity still not sufficient for design of effective algorithm ⇝ need further very technical property (developed by “reverse engineering”)

Def: continuous division L *constructive* ⇝

$$\forall \mathcal{T} \subset \mathbb{T}(X) \text{ finite}, \ t \in \mathcal{T}, \ y \in \bar{X}_{L,\mathcal{T}}(t) \text{ such that}$$

(i) $yt \notin \langle \mathcal{T} \rangle_L$

(ii) if $\exists\, s \in \mathcal{T}, \ z \in \bar{X}_{L,\mathcal{T}}(s) : zs \mid yt \wedge zs \neq yt$, then $zs \in \langle \mathcal{T} \rangle_L$

$$\nexists\, r \in \langle \mathcal{T} \rangle_L \ : \ yt \in \mathcal{C}_{L,\mathcal{T} \cup \{r\}}(r)$$

(underlying **idea**: it makes no sense in a completion process to add elements already contained in the involutive span)

Continuous and Constructive Divisions

Problem: continuity still not sufficient for design of effective algorithm $\rightsquigarrow$ need further very technical property (developed by “reverse engineering”)

Def: continuous division L *constructive* $\rightsquigarrow$

$$\forall\,\mathcal{T} \subset \mathbb{T}(X) \text{ finite, } t \in \mathcal{T},\ y \in \bar{X}_{L,\mathcal{T}}(t) \text{ such that}$$

$$\textbf{(i)}\quad yt \notin \langle \mathcal{T} \rangle_L$$

$$\textbf{(ii)}\quad \text{if } \exists\, s \in \mathcal{T},\ z \in \bar{X}_{L,\mathcal{T}}(s) : zs \mid yt \wedge zs \neq yt, \text{ then } zs \in \langle \mathcal{T} \rangle_L$$

$$\nexists\, r \in \langle \mathcal{T} \rangle_L\ :\ yt \in \mathcal{C}_{L,\mathcal{T}\cup\{r\}}(r)$$

Lemma: Janet and any continuous global division constructive

Proof: simple for global division; very technical for Janet division

Monomial Completion

Basic monomial completion algorithm

Input: finite set $\mathcal{T} \subset \mathbb{T}(X)$, involutive division L

Output: weakly involutive completion $\hat{\mathcal{T}}$ of $\mathcal{T}$

```
$\hat{\mathcal{T}} \leftarrow \mathcal{T}$
loop
    $\mathcal{S} \leftarrow \left\{ yt \mid t \in \hat{\mathcal{T}},\ y \in \bar{X}_{L,\hat{\mathcal{T}}}(t),\ yt \notin \langle \hat{\mathcal{T}} \rangle_L \right\}$
    if $\mathcal{S} = \emptyset$ then
        return $\hat{\mathcal{T}}$
    else
        choose $s \in \mathcal{S}$ such that $\mathcal{S}$ does not contain a proper divisor of it
        $\hat{\mathcal{T}} \leftarrow \hat{\mathcal{T}} \cup \{s\}$
    end if
end loop
```

Monomial Completion

Prop: $\mathcal{T}$ possesses weakly involutive completions, L constructive $\Longrightarrow$ algorithm terminates with a weakly involutive completion $\hat{\mathcal{T}}$

(Sketch of) Proof:

- *Correctness* obvious: upon termination $\hat{\mathcal{T}}$ locally involutive
- *Termination* proof very technical: use continuity of L to show that *each* added term lies in *any* involutive completion of $\mathcal{T}$ as otherwise contradiction to constructivity of L

Monomial Completion

- existence of (weakly) involutive completion must be *assumed*
  - ☐ very different to standard *Gröbner* theory (termination implies existence of basis!)
  - ☐ no issue for *Noetherian* division like Janet
- termination proof implies surprising properties of output
  - ☐ $\mathcal{T}_L$ *any* weakly involutive completion of $\mathcal{T}$ $\Longrightarrow$ $\hat{\mathcal{T}} \subseteq \mathcal{T}_L$
  - ☐ output *independent* of choices in Line 7 (simple way to implement choice: use term order)
- natural choice for input: *minimal* basis of $\langle \mathcal{T} \rangle$ (will see later $\rightsquigarrow$ yields *minimal involutive basis*)
- recall: simple elimination process yields *strong* involutive basis

Monomial Completion

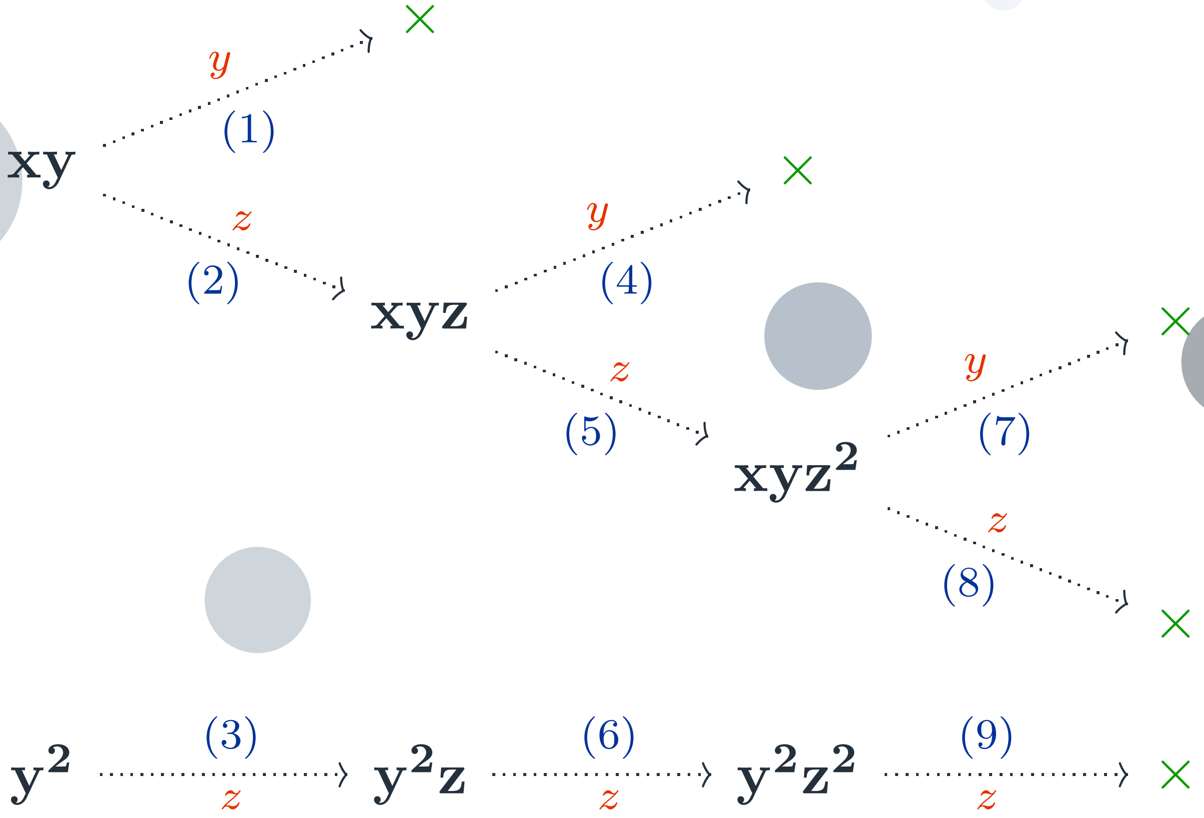
- existence of (weakly) involutive completion must be *assumed*
  - ☐ very different to standard *Gröbner* theory (termination implies existence of basis!)
  - ☐ no issue for *Noetherian* division like Janet
- termination proof implies surprising properties of output
  - ☐ $\mathcal{T}_L$ *any* weakly involutive completion of $\mathcal{T} \quad \Longrightarrow \quad \hat{\mathcal{T}} \subseteq \mathcal{T}_L$
  - ☐ output *independent* of choices in Line 7 (simple way to implement choice: use term order)
- natural choice for input: *minimal* basis of $\langle\mathcal{T}\rangle$ (will see later $\rightsquigarrow$ yields *minimal involutive basis*)
- recall: simple elimination process yields *strong* involutive basis

Lemma: $\mathcal{B}$ *minimal* basis of $\langle\mathcal{T}\rangle$, $L = P$ *Pommaret* division $\Longrightarrow$ no termination, if at some stage $\deg \hat{\mathcal{T}} > \deg \operatorname{lcm} \mathcal{B}$

Proof: consequence of syzygy theory in Lecture 5

Monomial Completion

Example: $\mathcal{T} = \{z^3, y^2, xy\}$ with Pommaret division
(choose in each iteration yt minimal for `degrevlex`)



$\mathbf{xy}$ $\xrightarrow{y}$ (1) ×
$\mathbf{xy}$ $\xrightarrow{z}$ (2) $\mathbf{xyz}$
$\mathbf{xyz}$ $\xrightarrow{y}$ (4) ×
$\mathbf{xyz}$ $\xrightarrow{z}$ (5) $\mathbf{xyz^2}$
$\mathbf{xyz^2}$ $\xrightarrow{y}$ (7) ×
$\mathbf{xyz^2}$ $\xrightarrow{z}$ (8) ×

$\mathbf{y^2} \xrightarrow[z]{(3)} \mathbf{y^2z} \xrightarrow[z]{(6)} \mathbf{y^2z^2} \xrightarrow[z]{(9)} \times$

Polynomial Completion

Given finite polynomial set $\mathcal{F} \subset \mathcal{P}$, term order $\prec$, involutive division L

Simplest approach:

- compute *Gröbner* basis $\mathcal{G}$ of $\mathcal{I} = \langle\mathcal{F}\rangle$ (e. g. with Buchberger algorithm)
  $\rightsquigarrow$ leading terms $\operatorname{lt}\mathcal{G}$ generate leading ideal $\operatorname{lt}\mathcal{I}$
- apply *monomial* completion algorithm to $\operatorname{lt}\mathcal{G}$
  (keeping full polynomials!)
- obtain (weakly) *involutive* basis $\mathcal{H} \supseteq \mathcal{G}$ of $\mathcal{I}$

Polynomial Completion

Given finite polynomial set $\mathcal{F} \subset \mathcal{P}$, term order $\prec$, involutive division L

Better approach:

- generalise *monomial* completion algorithm
- requires two subalgorithms
  - ☐ $\texttt{NormalForm}_{L,\prec}(g, \mathcal{H})$
    involutive normal form of polynomial $g \in \mathcal{P}$ wrt finite set $\mathcal{H} \subset \mathcal{P}$
  - ☐ $\texttt{(Head)AutoReduce}_{L,\prec}(\mathcal{H})$
    involutive (head) autoreduction of finite set $\mathcal{H} \subset \mathcal{P}$

(obtained by obvious modifications of standard algorithms)

Polynomial Completion

Basic polynomial completion algorithm

Input: finite set $\mathcal{F} \subset \mathcal{P}$, term order $\prec$, involutive division L

Output: involutive basis $\mathcal{H}$ of $\mathcal{I} = \langle \mathcal{F} \rangle$ wrt L and $\prec$

```
$\mathcal{H} \leftarrow \mathtt{HeadAutoReduce}_{L,\prec}(\mathcal{F})$
loop
    $\mathcal{S} \leftarrow \{yh \mid h \in \mathcal{H},\, y \in \bar{X}_{L,\mathcal{H},\prec}(h),\, yh \notin \langle \mathcal{H} \rangle_{L,\prec}\}$
    if $\mathcal{S} = \emptyset$ then
        return $\mathcal{H}$
    else
        choose $\bar{g} \in \mathcal{S}$ such that $\operatorname{lt} \bar{g} = \min_\prec \mathcal{S}$
        $g \leftarrow \mathtt{NormalForm}_{L,\prec}(\bar{g}, \mathcal{H})$
        $\mathcal{H} \leftarrow \mathtt{HeadAutoReduce}_{L,\prec}(\mathcal{H} \cup \{g\})$
    end if
end loop
```

Polynomial Completion

Theorem: division L constructive and Noetherian $\Longrightarrow$ algorithm terminates with involutive basis $\mathcal{H}$ of $\mathcal{I}$

Polynomial Completion

Theorem: division L constructive and Noetherian $\Longrightarrow$ algorithm terminates with involutive basis $\mathcal{H}$ of $\mathcal{I}$

(Sketch of) Proof:

- extend notion of *locally involutive set* to polynomial sets
- show that for continuous division any locally involutive and *involutively head autoreduced* set is involutive
- Noetherian argument shows that leading ideal $\langle \operatorname{lt} \mathcal{H} \rangle$ stabilises
- then polynomial completion reduces (more or less) to monomial completion

Polynomial Completion

Theorem: division L constructive and Noetherian $\Longrightarrow$ algorithm terminates with involutive basis $\mathcal{H}$ of $\mathcal{I}$

Some comments:

- it does *not* suffice to assume existence of involutive basis of $\mathcal{I}$ $\rightsquigarrow$ we need existence of involutive bases for *all subideals* of $\operatorname{lt}\mathcal{I}$
- choice in Line 7 corresponds to *normal selection strategy* $\rightsquigarrow$ use important for *termination* proof
- even if algorithm does *not* terminate, it always produces for term orders of type ω a *Gröbner* basis after a *finite* number of steps
- algorithm implicitly reduces S*-polynomials*
- algorithm usually more efficient than *Buchberger algorithm*
  - ☐ *Buchberger criteria* to large extent *automatically “built-in”*
  - ☐ implicitly *“Hilbert driven”* (without a priori knowledge of Hilbert function!)

Polynomial Completion

Example: $\mathcal{P} = \mathbb{k}[x, y]$, Pommaret division P

$$\mathcal{F} = \{\mathbf{f}_1 = y^2\mathbf{e}_1,\ \mathbf{f}_2 = xy\mathbf{e}_1 + \mathbf{e}_2,\ \mathbf{f}_3 = x\mathbf{e}_2\} \subset \mathcal{P}^2$$

Polynomial Completion

Example: $\mathcal{P} = \Bbbk[x,y]$, Pommaret division P

$$\mathcal{F} = \{\mathbf{f}_1 = y^2\mathbf{e}_1,\ \mathbf{f}_2 = xy\mathbf{e}_1 + \mathbf{e}_2,\ \mathbf{f}_3 = x\mathbf{e}_2\} \subset \mathcal{P}^2$$

- choose term order such that $xy\mathbf{e}_1 \succ \mathbf{e}_2$ $\rightsquigarrow$ $\langle \operatorname{lt} \mathcal{F}\rangle$ has *no* finite Pommaret basis (consider $\mathbf{e}_2$-component)
- add S-“polynomial” $\mathbf{S}(\mathbf{f}_1, \mathbf{f}_2) = y\mathbf{e}_2 = \mathbf{f}_4$ $\rightsquigarrow$

$$\mathcal{H} = \mathcal{F} \cup \{\mathbf{f}_4\}$$ *finite* Pommaret basis of $\langle\mathcal{F}\rangle$

Polynomial Completion

Example: $\mathcal{P} = \Bbbk[x, y]$, Pommaret division P

$$\mathcal{F} = \{\mathbf{f}_1 = y^2\mathbf{e}_1,\ \mathbf{f}_2 = xy\mathbf{e}_1 + \mathbf{e}_2,\ \mathbf{f}_3 = x\mathbf{e}_2\} \subset \mathcal{P}^2$$

- choose term order such that $xy\mathbf{e}_1 \succ \mathbf{e}_2$ $\rightsquigarrow$ $\langle \operatorname{lt} \mathcal{F} \rangle$ has *no* finite Pommaret basis (consider $\mathbf{e}_2$-component)
- add S-"polynomial" $\mathbf{S}(\mathbf{f}_1, \mathbf{f}_2) = y\mathbf{e}_2 = \mathbf{f}_4$ $\rightsquigarrow$

$\mathcal{H} = \mathcal{F} \cup \{\mathbf{f}_4\}$ *finite* Pommaret basis of $\langle \mathcal{F} \rangle$

- termination of completion algorithm depends on properties of term order
  - ☐ take *"POT"* order with $s\mathbf{e}_1 \succ t\mathbf{e}_2$ for arbitrary $s, t \in \mathbb{T}(x, y)$ $\Longrightarrow$ *no termination*
  - ☐ take *"TOP"* order based on degree compatible order $\rightsquigarrow$ after finite number of iterations $\mathbf{f}_4$ is found $\Longrightarrow$ *termination*

Minimal Bases

Def: $\mathcal{I} \subseteq \mathcal{P}$, $\mathcal{H} \subset \mathcal{I}$ involutive basis

- $\mathcal{H}, \mathcal{I}$ monomial; $\mathcal{H}$ *minimal involutive basis* of $\mathcal{I}$ $\leadsto$ every monomial involutive basis $\hat{\mathcal{H}}$ of $\mathcal{I}$ satisfies $\mathcal{H} \subseteq \hat{\mathcal{H}}$
- $\mathcal{H}, \mathcal{I}$ polynomial; $\mathcal{H}$ *minimal involutive basis* of $\mathcal{I}$ $\leadsto$ $\operatorname{lt}\mathcal{H}$ minimal involutive basis of $\operatorname{lt}\mathcal{I}$

Minimal Bases

Def: $\mathcal{I} \subseteq \mathcal{P}$, $\mathcal{H} \subset \mathcal{I}$ involutive basis

- $\mathcal{H}, \mathcal{I}$ monomial; $\mathcal{H}$ *minimal involutive basis* of $\mathcal{I}$ $\rightsquigarrow$ every monomial involutive basis $\hat{\mathcal{H}}$ of $\mathcal{I}$ satisfies $\mathcal{H} \subseteq \hat{\mathcal{H}}$
- $\mathcal{H}, \mathcal{I}$ polynomial; $\mathcal{H}$ *minimal involutive basis* of $\mathcal{I}$ $\rightsquigarrow$ $\operatorname{lt}\mathcal{H}$ minimal involutive basis of $\operatorname{lt}\mathcal{I}$

Prop: $\mathcal{I} \subset \mathcal{P}$ monomial ideal with involutive basis $\Longrightarrow$ minimal involutive basis exists and obtained by applying monomial completion algorithm to minimal basis in ordinary sense

Prop: L globally defined division $\Longrightarrow$ monomial involutive basis unique and thus minimal

Minimal Bases

Def: $\mathcal{I} \subseteq \mathcal{P}$, $\mathcal{H} \subset \mathcal{I}$ involutive basis

- $\mathcal{H}, \mathcal{I}$ monomial; $\mathcal{H}$ *minimal involutive basis* of $\mathcal{I}$ $\rightsquigarrow$ every monomial involutive basis $\hat{\mathcal{H}}$ of $\mathcal{I}$ satisfies $\mathcal{H} \subseteq \hat{\mathcal{H}}$
- $\mathcal{H}, \mathcal{I}$ polynomial; $\mathcal{H}$ *minimal involutive basis* of $\mathcal{I}$ $\rightsquigarrow$ $\operatorname{lt} \mathcal{H}$ minimal involutive basis of $\operatorname{lt} \mathcal{I}$

Example: $\mathcal{F} = \{x, x^2\} \subset \Bbbk[x]$

$\mathcal{F}$ *Janet* autoreduced (x non-mult. for x because of x^2) $\Longrightarrow$ algorithms will leave $\mathcal{F}$ unchanged

obviously: $\{x\}$ minimal involutive basis of $\langle \mathcal{F} \rangle$

Minimal Bases

Def: $\mathcal{I} \subseteq \mathcal{P}$, $\mathcal{H} \subset \mathcal{I}$ involutive basis

- $\mathcal{H}, \mathcal{I}$ monomial; $\mathcal{H}$ *minimal involutive basis* of $\mathcal{I}$ $\rightsquigarrow$ every monomial involutive basis $\hat{\mathcal{H}}$ of $\mathcal{I}$ satisfies $\mathcal{H} \subseteq \hat{\mathcal{H}}$
- $\mathcal{H}, \mathcal{I}$ polynomial; $\mathcal{H}$ *minimal involutive basis* of $\mathcal{I}$ $\rightsquigarrow$ $\operatorname{lt} \mathcal{H}$ minimal involutive basis of $\operatorname{lt} \mathcal{I}$

Prop: monic, involutively autoreduced, minimal involutive basis unique

Prop: L constructive, Noetherian division $\Longrightarrow$ every polynomial ideal $\mathcal{I} \subseteq \mathcal{P}$ has minimal involutive basis

Proof: optimised completion algorithm

Minimal Bases

Algorithm for minimal involutive basis ("$\mathcal{T}$-$\mathcal{Q}$ algorithm")

Input: finite set $\mathcal{F} \subset \mathcal{P}$, term order $\prec$, involutive division L

Output: minimal involutive basis $\mathcal{H}$ of $\mathcal{I} = \langle \mathcal{F} \rangle$ wrt L and $\prec$

```
$\mathcal{T} \leftarrow \emptyset$;   $\mathcal{Q} \leftarrow \mathcal{F}$
repeat
    $g \leftarrow 0$
    while $(\mathcal{Q} \neq \emptyset) \wedge (g = 0)$ do
        choose $f \in \mathcal{Q}$ such that $\operatorname{lt} f = \min_{\prec} Q$
        $\mathcal{Q} \leftarrow \mathcal{Q} \setminus \{f\}$;   $g \leftarrow \mathtt{NormalForm}_{L,\prec}(f, \mathcal{T})$
    end while
    if $g \neq 0$ then
        $\mathcal{T}' \leftarrow \{h \in \mathcal{T} \mid \operatorname{lt} g \prec \operatorname{lt} h\}$;   $\mathcal{T} \leftarrow (\mathcal{T} \setminus \mathcal{T}') \cup \{g\}$
        $\mathcal{Q} \leftarrow \mathcal{Q} \cup \mathcal{T}' \cup \{yh \mid h \in \mathcal{T},\ y \in \bar{X}_{L,\mathcal{T},\prec}(h)\}$
    end if
until $\mathcal{Q} = \emptyset$
return $\mathcal{T}$
```

Minimal Bases

Theorem: division L constructive and Noetherian $\Longrightarrow$ algorithm terminates with minimal involutive basis $\mathcal{H}$ of $\mathcal{I}$

Proof:

- *termination* proof requires only slight modifications
- $\mathcal{H}$ *involutive* basis essentially as before
- proof of *minimality* requires analysis of last time a generator is moved to $\mathcal{H}$

Minimal Bases

Theorem: division L constructive and Noetherian $\Longrightarrow$ algorithm terminates with minimal involutive basis $\mathcal{H}$ of $\mathcal{I}$

Proof:

- *termination* proof requires only slight modifications
- $\mathcal{H}$ *involutive* basis essentially as before
- proof of *minimality* requires analysis of last time a generator is moved to $\mathcal{H}$

Example: $\mathcal{F} = \{x, x^2\} \subset \Bbbk[x]$, Janet division

1. iteration: $\mathcal{T} = \{x\}$, $\mathcal{Q} = \{x^2\}$

2. iteration: $\mathcal{T} = \{x\}$, $\mathcal{Q} = \emptyset$

Optimisations and Complexity Issues

It's easy to implement a completion algorithm,
but difficult to provide a good implementation!

- *worst case* complexity of **any** algorithm for Gröbner bases is *doubly exponential* ⇝ potential *size* of basis (sharp estimate!)
- fortunately in practice rarely realised ⇝ "geometric" ideals have usually a lower *Castelnuovo-Mumford regularity* (see Lecture 5)
- good implementations require many *optimisations* of basic algorithms (proof of correctness often much more difficult)
- often only *heuristic* statements possible ⇝ good implementations provide *options* to control behaviour of algorithms
- important example: *selection strategy*

Optimisations and Complexity Issues

“Involutive Buchberger criteria”

- try to *predict* that a non-multiplicative product yh (involutively) reduces to 0 (reductions are the most expensive part of a completion!)
- here much less an issue than for *Buchberger algorithm*
  - ⇝ yields only a modest gain in computation time
- to a large extent automatically built-in in our completion algorithm
  - ⇝ consequence of *syzygy theory* (Lecture 5)

Optimisations and Complexity Issues

“Involutive Buchberger criteria”

- try to *predict* that a non-multiplicative product yh (involutively) reduces to 0 (reductions are the most expensive part of a completion!)
- here much less an issue than for *Buchberger algorithm*
  ⇝ yields only a modest gain in computation time
- to a large extent automatically built-in in our completion algorithm
  ⇝ consequence of *syzygy theory* (Lecture 5)

Remark: “value” of reductions to 0 depends on application context:

- we only need *some* Gröbner basis for, say, deciding an ideal membership problem ⇝ such reductions a waste of time
- we also need *syzygy module* (common in algebraic geometry) ⇝ (some) reductions to 0 yield valuable information on syzygies (Schreyer theorem — see Lecture 5)

Optimisations and Complexity Issues

“Involutive trees”

- **Problem:** fast determination of *multiplicative variables* for generators and fast search for *involutive divisors* important for effecient completion
- most studied for *Janet division*
- natural *tree structure* on subsets $(d_k, \dots, d_n) \subset \mathcal{T}$ used for definition of Janet division induced by inclusion relation $\rightsquigarrow$ leaves are elements of $\mathcal{T}$
- leads to special relationship with *lexicographic order* (leaves appear automatically sorted)
- refined version based on *binary trees*
- yields efficient *graph theoretic* algorithms (also for *maintaining* tree during completion!)

Optimisations and Complexity Issues

“Good Book-Keeping”

- keep track of *history* of generators in order to avoid redundancies
  - ☐ **Example:** for Pommaret division in $\mathbb{k}[x,y,z]$
    current basis contains $f \in \mathbb{k}[x]$ ⇝ must treat yf and zf ⇝
    assume both polynomials must be added unchanged to basis
    (both of class 1) ⇝ must later treat *both* $z(yf)$ *and* $y(zf)$
  - ☐ in $\mathcal{T}$-$\mathcal{Q}$ algorithm for minimal basis generator may repeatedly move between $\mathcal{T}$ and $\mathcal{Q}$ ⇝ record which non-multiplicative products have already been considered
- allows for simple extraction of *reduced Gröbner basis*
  (without any further computations!)

Optimisations and Complexity Issues

“Intermediate Expression Swell”

Problem: in- and output *small*, but intermediate results very *large* (quite common in computer algebra)

Example: (Arnold) $\mathcal{P} = \mathbb{Q}[x, y, z]$, `degrevlex`

$$f_1 = 8y^2z^2 + 5y^3z + 3xz^3 + xyz^2 \qquad f_3 = 8z^3 + 12y^3 + x^2z + 3$$
$$f_2 = z^5 + 2x^2y^3 + 13x^3y^2 + 5x^4y \qquad f_4 = 7y^4z^2 + 18x^2y^3z + x^3y^3$$

reduced Gröbner basis of $\mathcal{I} = \langle f_1, f_2, f_3, f_4 \rangle$

$$g_1 = z \qquad g_2 = y^3 + 1/4 \qquad g_3 = x^2$$

intermediate polynomials have coefficients with about 80.000 digits

Janet basis requires additionally: $g_4 = x^2y$, $g_5 = x^2y^2$
largest intermediate coefficients have about 400 digits